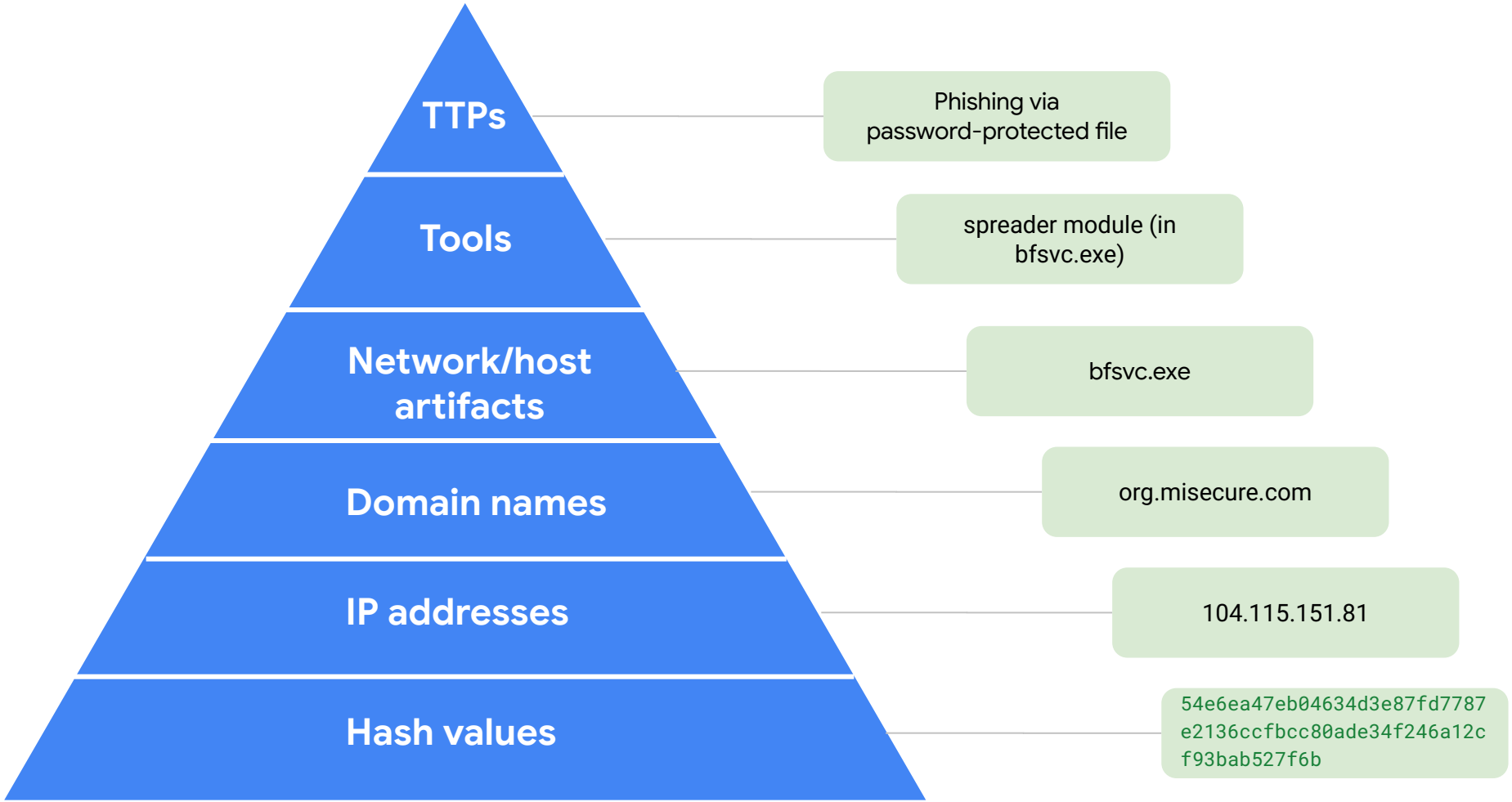
Has this file been identified as malicious? Explain why or why not.

- Yes, this file has been identified as malicious.
- According to VirusTotal, 58 out of 72 security vendors flagged this file as malicious. This is a strong indicator that this file is malware that contains a trojan or backdoor.
- Additionally, the time of attack showed that unauthorized executable files were created shortly after the employee opened the file, and the intrusion detection system triggered an alert a minute later. This supports the conclusion that this file is malicious and harmful.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Phishing via password-protected file
spreader module (in bfsvc.exe)
bfsvc.exe
org.misecure.com
104.115.151.81
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

***three* indicators of compromise (IoCs) that are associated with this file hash**

1. A weird `.exe` file like `bfsvc.exe`
2. weird IP address and Domain Name `org.misecure.com`
3. Hash value indicator: `54e6ea47eb04634d3e87fd7787e2136ccfbc80ade34f246a12cf93bab527f6b`